EXHIBIT 6

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF TENNESSEE

```
----------------------------------------------------------- x
                                                            :
SNMP RESEARCH, INC. and SNMP                                :      Case No. 3:20-cv-00451-CEA-DCP
RESEARCH INTERNATIONAL, INC.,                               :
                                                            :
                              Plaintiffs,                   :
                                                            :
                    v.                                      :
                                                            :
BROADCOM INC.; BROCADE                                      :
COMMUNICATIONS SYSTEMS LLC; and                             :
EXTREME NETWORKS, INC.,                                     :
                                                            :
                              Defendants.                   :
----------------------------------------------------------- X
```

DECLARATION OF DANIEL DEBACKER IN SUPPORT OF EXTREME NETWORKS, INC.'S BRIEF REGARDING SOURCE CODE INSPECTION

I, Dan DeBacker, declare and attest as follows:

1.   I am VP Service Provider Product Management & Engineering at Extreme Networks, Inc. ("Extreme"), a defendant in this action. I have personal knowledge of the facts set forth in this Declaration and can and will testify thereto under oath if called to do so.

A. The Inspection Products

2.   I understand that Extreme was to provide source code in this action for the products listed in paragraph 49 of the Complaint from January 1, 2017 to present by April 22, 2022.

3.   I was personally involved in the collection of source code for these products.

4.   I also included in the collection three additional products that are not listed in the Complaint. Those products are SLX 9740, Extreme 8720, and Extreme 8520. I will refer to the products listed in paragraph 49 of the Complaint and these three additional products as the "Inspection Products."

5.   From January 1, 2017 to March 2022, Extreme issued approximately 251 releases for the Inspection Products. This includes approximately 104 mainline releases and 147 customer-specific releases.

6.   I estimate the size of these releases to total more than 12 terabytes of data.

7.   To put this size into context, in my thirty-three year career, I have never been involved in exporting that amount of data. In fact, while at Extreme, I have never been involved in exporting source code at all to anyone outside of Extreme's engineering department.

8.   Extreme stores the source code for its releases in different repositories. The majority of the code for the Inspection Products is stored in ClearCase repositories. The remainder of the code is stored in Github repositories.

9.   These repositories do not just contain the source code for the Inspection Products; rather, these repositories also include source code for hundreds of other products and projects.

B. Extreme's Preparation of Source Code for the Inspection Products

10.   To make approximately 12 terabytes of source code available in this action, I and my team followed the process described below.

11.   My team first created snapshots of each release from the code repositories (both ClearCase and Github repositories).

12.   We then created tarballs of each release available. Tarballs provide a way to compress a large number of files into one archive.

13.   The next step was to transfer the tarballs from the repositories located outside of California to our company servers in San Jose, California. There is only one data pipe between the site holding the source code and our servers in San Jose. That means that the transfer of data

2

from Extreme's offsite location to San Jose had a maximum speed capped by the data pipeline, taking into account Extreme's normal day to day activities using the data pipeline.

14.   Once the data was in San Jose, we made that data available in this litigation in three different forms.

15.   First, tarballs for all releases available to Extreme were loaded to Extreme's servers located in San Jose. I note that Extreme was unable to access approximately 11 customer-specific releases, and so tarballs for these releases were not included on the servers or otherwise. When I say that Extreme is unable to access 11 customer-specific releases, to be clear, I do not mean that we are capable of accessing such information but are in some way (e.g., a confidentiality contract) prohibited from doing so. I mean that we are quite literally and as a technical matter unable to access this information.

16.   Second, releases for the Inspection Products that were originally in ClearCase were made available through ClearCase. To make these releases available without providing access to other products in the repositories, my team devoted manpower to creating scripts to generate "views" of the releases of the Inspection Products.

17.   Third, we loaded a subset of the releases of the Inspection Products to external drives. We were unable to load all files to the external drive by April 22, but we uploaded all that we were able to do with timing and technology constraints.

18.   This third category was particularly time-consuming. To speed up this step, we wrote scripts to automate the process and ran processes in parallel. Nevertheless, this step involved **_hundreds_** of hours by Extreme engineers.

19. In total, I am aware of at least eight Extreme employees or contractors involved in the preparation of source code for the inspection. This includes individuals from California to Canada to India.

20. Extreme's employees worked, literally, around the clock to make the source code for the Inspection Products available.

C. Source Code Computers Available for the Inspection

21. Two laptops were provided at Extreme's San Jose offices for the April 22 inspection in this action.

22. Both of those laptops had access to Extreme's servers and ClearCase.

23. At least one of the laptops also had access to the external drive with the subset of the releases loaded on that drive.

D. MD5 Checksums

24. I understand that the Protective Order in this case calls for manifests with "MD5 checksum (or stronger) in native form of every source and executable file on the Source Code Computers."

25. Extreme does not create or keep MD5 checksums for the source code for the releases of the Inspection Products in the ordinary course of business. In other words, Extreme does not possess MD5 checksum (or stronger) in native form of any source or executable files that were made available on the laptops.

26. I estimate that it would take multiple months to generate checksum values for all files within each release.

27. This process would require Extreme to create approximately 75 million files. That is because there are approximately 300,000 files for each release. As noted above, there are

4

approximately 251 releases. That leads to approximately 75 million files that Extreme made available by the source code computers, each of which would require the generation of a new MD5 checksum.

28.   To my knowledge, the utility of MD5 checksum values is to verify the integrity of downloads. Extreme does not use MD5 checksum values on any source code in the ordinary course of business because there is no utility of these values in this context to Extreme.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 4, 2022 in Bigfork, Montana.

_____
Daniel DeBacker